Software Version 1.5
Version 1.2

Xerox Mobile Print Solution

Information Assurance Disclosure

Table of Contents

Contents

[This page left intentionally blank]

1.0 Introduction

A Xerox Workflow Solution that connects a corporation mobile workforce to new productive ways of printing. Printing is easy and convenient from any mobile device without needing standard drivers and cables.

1.1 Purpose

The purpose of this document is to disclose information for the Xerox Mobile Print Solution with respect to system security. *System Security,* for this paper, is defined as how print jobs are received, accessed, and transmitted, how user information is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. Please note that the customer is responsible for the security of their network and the Mobile Print product does not establish security for any network environment.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the Xerox Mobile Print Solution relative to Information Assurance (IA).

This document does NOT provide tutorial level information about security, connectivity, PDLs, or Xerox Mobile Print Solution features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

1.2 Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

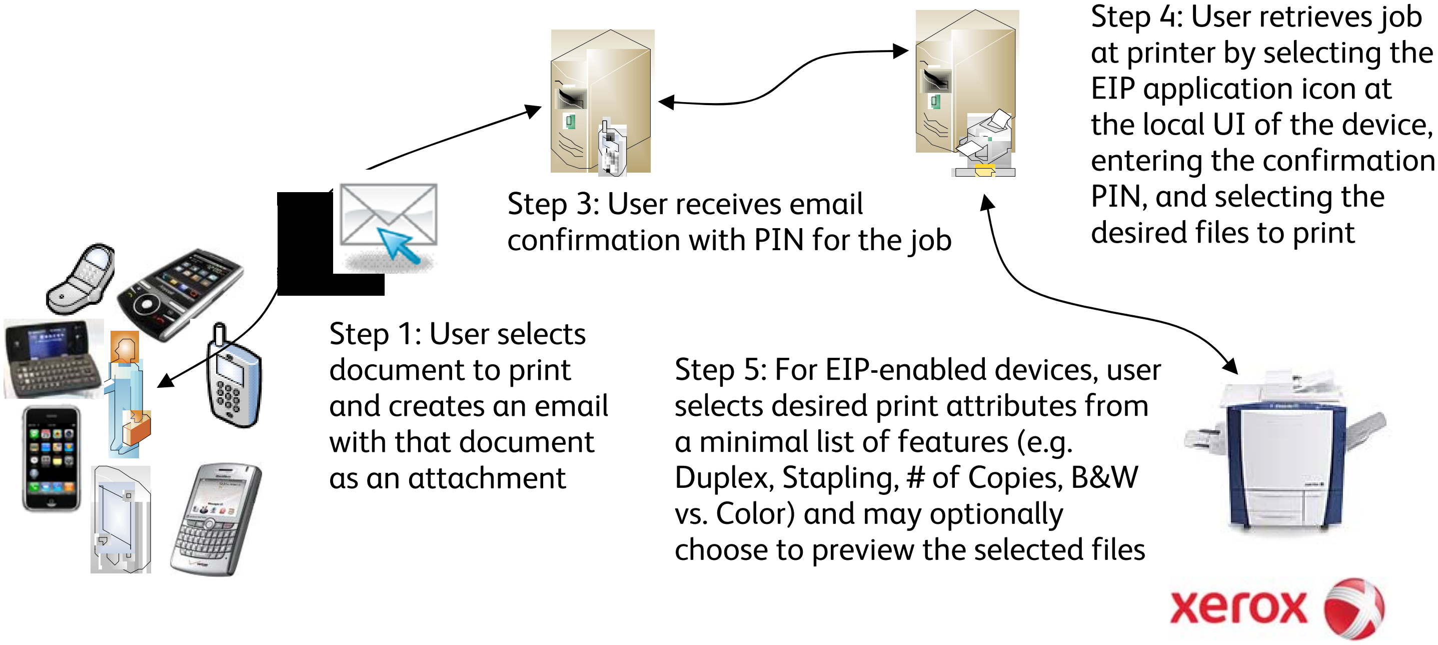
1.3 Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.

Xerox Mobile Print Solution Workflow

Document Types:

- Microsoft Office documents
- Print Ready files (PDF, XPS, TIFF)
- Photos (JPEG)
- The actual email (text)



Step 1: User selects document to print and creates an email with that document as an attachment

Step 2: Email is received at email server and is retrieved by the EIP application running on the customer’s server

Step 3: User receives email confirmation with PIN for the job

Step 4: User retrieves job at printer by selecting the EIP application icon at the local UI of the device, entering the confirmation PIN, and selecting the desired files to print

Step 5: For EIP-enabled devices, user selects desired print attributes from a minimal list of features (e.g. Duplex, Stapling, # of Copies, B&W vs. Color) and may optionally choose to preview the selected files

2.1 Security-Relevant Subsystems

The security considerations are two-fold, first the security of the customer’s documents during transport and storage on multiple servers, and second the security of the Xerox Mobile Print Solution configuration which includes customer user account information. As one can see from the above diagram their document travels through multiple servers over a combination of wireless and wired networks. All of which use normal, industry- standard technologies incorporating built-in security capabilities. These capabilities do need to be enabled, and the choice of which are used are up to the customers IT department. This section captures the security considerations and implementation of Mobile Print 1.5 in the following areas:

- Customer Supplied Network.
- User and Email Server Communication.
- Email Server and Mobile Print Server Communication.
- Mobile Print Server and the Multi-Function Devices (MFD) Communication.
- Mobile Print Server Administration.

- Microsoft SQL Server Express database deployment.
- Mobile Print Server Windows NTFS file structure permissions

2.2 Customer Supplied Network

Computer/Information Security is a journey and not a destination. Even the most secure systems are vulnerable to someone who has the right knowledge, access, and enough time. Threats include physical damage at the system, over networks, or as well as damage caused by viruses. The goal is to minimize the security risks as much as possible, and have policies in place to detect and reduce the negative impact of a security incident. Examples of things that can be done to reduce risks include proper use of logins and passwords, restricting network access, and the use of virus detection software.

Mobile Print Security

Xerox's Role

Xerox will strive to provide the most secure software product possible based on the information and technologies available while maintaining the products performance, value, functionality, and productivity.

Xerox will:

- Run industry standard security diagnostics tests during development to determine vulnerabilities. If found, the vulnerabilities will either be fixed, minimized, or documented
- Monitor, notify, and supply (when necessary) security patches provided by third party software vendors used with the Mobile Print software.

Customer's Role

Although the Mobile Print product support team will try to provide software that is secure, the customer is ultimately responsible for securing their environment to meet their specific security needs. Depending on the customer needs, the customer can increase security by installing a firewall, implementing a private network, and/or physically securing the hardware to a limited access area. The customer, depending on their needs, should use tools to monitor and log physical and network access to the Mobile Print hardware and software to determine if and when a security incident has occurred. The customer should also back-up their data to ensure that is may be recovered in case of deletion or corruption.

In implementing a security strategy, customers must keep in mind that they should not modify the Mobile Print product system or its environment in any way that will prevent it from functioning properly. If the customer performs such modifications, Xerox will not be able to support the product should problems occur. The customer may be responsible for returning the Mobile Print product back to the original installed state. This may include uninstalling unsupported software, resetting configuration settings, or possibly reinstalling the Mobile Print software product.

2.3 User and Email Server Communication

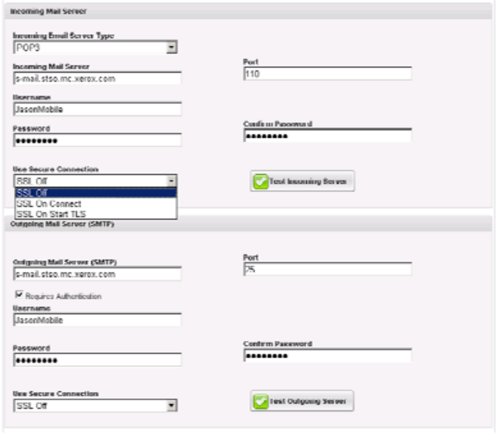
Users submit their documents for printing using standard email messages from their smart phone to their company's Email Server. Whether the email messages are encrypted or not, is a decision and responsibility of the company's IT department.

The Mobile Print Server does communicate to the end user via email messages sent through the customer's Email Server (described in section 2.4). Each time a user submits documents for printing; the Mobile Print Server will retrieve the message and respond with a confirmation email message. The confirmation email message contains a personal confirmation code. The confirmation code is later used to retrieve and print their documents at the Multi-Function Device (MFD) (see section 2.5)

Confirmation codes are 6 digit random numbers unique to each user email address. Once assigned the confirmation code will be reused for each submission from the same user. Note, this is specifically for the users convenience so that all their jobs will be shown at the MFD. Users may request that their confirmation code be changed at any time.

2.4 Email Server and Mobile Print Server Communication

Network communication between the email server and the Mobile Print Server is configured within the administration pages.



Incoming Mail Server

Incoming Email Server Type: POP3

Incoming Mail Server: s-mail.stso.mc.xerox.com

Port: 110

Username: JasonMobile

Password: ••••••••

Confirm Password: ••••••••

Use Secure Connection: SSL Off

Outgoing Mail Server (SMTP)

Outgoing Mail Server (SMTP): s-mail.stso.mc.xerox.com

Port: 25

☑ Require Authentication

Username: JasonMobile

Password: ••••••••

Confirm Password: ••••••••

Use Secure Connection: SSL Off

For security:

1. The Mobile Print server will require a customer supplied username and password to access the Mail Server. The credentials are stored within the SQL Express database.
2. The communication port is configurable.
3. Network communication between the servers can be configured to be encrypted using SSL.

2.5 Mobile Print Server and Multi-Function Device (MFD) Communication.

When users are ready to print their documents, they will go to a Multi-Function Device (MFD), start and EIP application, and enter their confirmation code.

The EIP application is a web based application using standard HTTP or HTTPS communication to the Mobile Print Server.

During MFD registration, Mobile Print will initially communicate to the MFD using HTTP, but will configure the MFD for HTTPS communication.

2.6 Administrator configuration and usage of the Mobile Print Server.

Accessing the Mobile Print server administration web pages use the HTTP or HTTPS specifications for Basic Authentication. This access protocol requires a username and password for client authentication and is supported my most browsers.

During installation the MPAdmin group is created.

Windows user accounts that are members of the Administrators or MPAdmin groups would have access, but not user accounts.

2.7 Microsoft SQL Server Express database deployment.

During installation of the Mobile Print server, Microsoft SQL Server Express is installed for storing configuration information and runtime data. Use of the database is restricted to the Mobile Print server software and cannot be shared with other applications.

The Mobile Print installer will:

1. Disable the default database SA account.
2. Per industry standard practices; create a database owner account which is mapped to the IIS created Network Services account. Thus the database can only be accessed via IIS.

Note: Members of the Windows Administrators group, by design, do have access to the database..

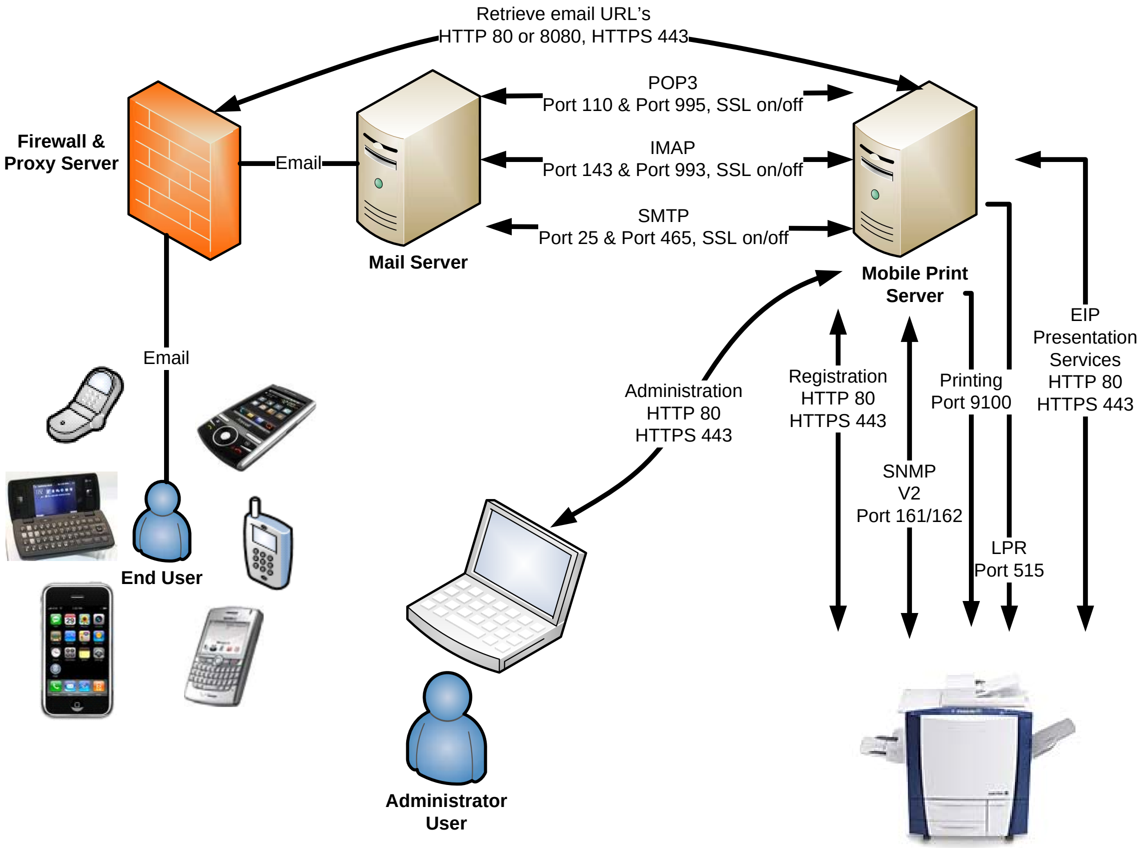
2.8 Mobile Print Server Windows NTFS file structure permissions

The Mobile Print Server stores files within the Windows NTFS file structure. The locations and the access permissions are shown below:

Directory	Administrator Group	Network Services User	Users Group	MPAdmin Group	System User
\(Root)					
\AdminApplication	Full Control	Read, Execute, List		Full Control	Full Control
\AdminApplication\bin\ MPLicenseUpgradeTool.exe	Full Control	Read, Execute, List	Read, Execute, List	Full Control	Full Control
\AdminPrinterDisplay	Full Control	Read, Execute, List		Full Control	Full Control
\AppData\XeroxMobilePrint	Full Control	Read, Execute, List	Full Control	Full Control	Full Control
\Data	Full Control	Read, Execute, List		Full Control	Full Control
\EIP	Full Control	Read, Execute, List	Read, Execute, List		
\EIP\Logs	Full Control	Full Control	Read, Execute, List	Full Control	Full Control
\InstallerSupport	Full Control	Read, Execute, List		Full Control	Full Control
\License	Full Control	Read, Execute, List		Full Control	Full Control
\Log	Full Control	Read, Execute, List		Full Control	Full Control
\Services	Full Control	Read, Execute, List		Full Control	
\Services\DCE\Logs	Full Control	Read, Execute, List		Full Control	Full Control
\Working	Full Control	Full Control		Full Control	Full Control
\xrxsite.url	Full Control		Read, Execute, List	Full Control	Full Control

2.9 Xerox Mobile Print Solution Network Diagram

The Xerox Mobile Print Solution Network Diagram showing protocols and typical port numbers. Port numbers are configurable.


Retrieve email URL's
HTTP 80 or 8080, HTTPS 443
POP3
Port 110 & Port 995, SSL on/off
IMAP
Port 143 & Port 993, SSL on/off
SMTP
Port 25 & Port 465, SSL on/off
Firewall &
Proxy Server
Email
Mail Server
Mobile Print
Server
Email
End User
Administration
HTTP 80
HTTPS 443
Registration
HTTP 80
HTTPS 443
SNMP
V2
Port 161/162
Printing
Port 9100
LPR
Port 515
EIP
Presentation
Services
HTTP 80
HTTPS 443
Administrator
User